Abstract

Various embodiments are provided relating to security of a computer, namely, a security software product, a computer-readable medium, a computerized method, and a computer security system. Illustrative is one embodiment of a security software product for use on a host computer to monitor for, and respond to, activity corresponding to a rootkit exploitation which renders the host computer's operating system insecure. The security software product comprises computer readable media having a suite of interfaced software components, such as loadable kernel modules. An exploitation detection component detects the activity corresponding to the rootkit exploitation. A forensics data collection component collects forensics data characteristic of the rootkit exploitation so that it may be transferred to a removable storage device. An OS restoration component restores the operating system to a secure condition in response to detection of the exploit.